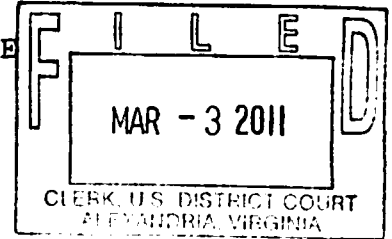


IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



TECSEC, INC.

Plaintiff,

v.

1:10cv115 (LMB/TCB)

INTERNATIONAL BUSINESS MACHINES  
CORP., et al.,

Defendants.

MEMORANDUM OPINION

Before the Court are the parties' cross-motions for summary judgment concerning plaintiff's allegations of patent infringement by the defendant, International Business Machines Corporation [Dkt. Nos. 462 and 478]. For the reasons stated in this Memorandum Opinion, the defendant's Motion for its Proposed Claim Constructions and Summary Judgment of No Infringement [Dkt. No. 462] has been granted, the remainder of plaintiff's Motion for Partial Summary Judgment of Infringement by Defendant IBM and on Defendant's Affirmative Defenses of Release and Immunity under 28 U.S.C. § 1498 [Dkt. No. 478] has been denied,<sup>1</sup> and summary judgment will now be entered in favor of the defendant on all claims asserted in plaintiff's Second Amendment Complaint.

---

<sup>1</sup> On February 10, 2011, the portion of plaintiff's motion seeking summary judgment on defendant's affirmative defenses of release and immunity under 28 U.S.C. § 1498 was denied. On February 25, 2011, the remainder of plaintiff's motion was denied, and defendant's motion was granted in full. This Memorandum Opinion explains the reasoning for the Court's February 25, 2011 Order.

### I. Background

The plaintiff in this patent infringement action, TecSec, Inc. ("TecSec"), is a Virginia corporation with its principal place of business in McLean, Virginia. TecSec's primary business is the development of encryption and security techniques; it has designed, developed, and sold a number of cryptography and security-related products since its founding in 1990, and has been awarded more than thirty United States patents in the field of encryption. See Pl.'s Second Amend. Compl. ¶¶ 20-25.

In this civil action, TecSec asserts that defendant International Business Machines Corporation ("IBM") and several other defendants have infringed one or more of the claims of six of its patents, in violation of 35 U.S.C. § 271 et seq.<sup>2</sup> TecSec's Second Amended Complaint, filed on July 6, 2010, asserts infringement of the following three groups of patents:

1. United States Patent No. 5,369,702 ("the '702 patent"), issued on November 29, 1994; United States Patent No. 5,680,452 ("the '452 patent"), issued on October 21, 1997; United States Patent No. 5,717,755 ("the '755 patent"), issued on February 10, 1998; and United States Patent No. 5,898,781 ("the '781 patent"), issued on April 27, 1999. All four patents deal with the "Distributed Cryptographic Object Method" for data encryption and are collectively referred to as "the DCOM

---

<sup>2</sup> The Second Amended Complaint names IBM, SAS Institute, Inc., SAP America, Inc., SAP AG, Cisco Systems, Inc., Oracle America, Inc., Sybase, Inc., Software AG, Inc., Software AG, Adobe Systems Incorporated, eBay Inc., PayPal Inc., and Oracle Corporation as defendants. However, in an Order dated June 4, 2010, the litigation was stayed as to all defendants except IBM and eBay, Inc., and the Second Amended Complaint was dismissed without prejudice as to defendant eBay on August 27, 2010. Accordingly, only the claims against defendant IBM are presently at issue.

patents" or "the '702 patent family."

2. United States Patent No. 6,694,433 ("the '433 patent"), issued on February 17, 2004, dealing with an "Extensible Markup Language (XML) encryption scheme," and alternatively referred to as "the XML patent."

3. United States Patent No. 7,069,448 ("the '448 patent"), issued on June 27, 2006, dealing with "Context Oriented Crypto-Processing on a Parallel Processor Array," and alternatively referred to as "the Parallel Processor patent."

Id. ¶ 1. In particular, TecSec accuses IBM of infringing 25 claims of the six patents in suit, including:

1. The '702 patent: claims 2, 8, 9, 12, 14, and 15<sup>3</sup>
2. The '452 patent: claims 1, 2, and 13
3. The '755 patent: claims 1 and 2
4. The '781 patent: claims 1, 2, 3, 10, 13, 14, and 15
5. The '433 patent: claims 1, 3, 4, 8, and 12<sup>4</sup>
6. The '448 patent: claims 1 and 5

See id.; see also IBM's Br. in Supp. of its Proposed Claim Constructions and Mot. for Summ. J. of No Infringement ["Def.'s Mot. for Summ. J."] at 1. As a result of the alleged infringement, plaintiff seeks relief in the form of a permanent injunction enjoining the defendant and all of its affiliates from infringing the patents-in-suit, along with an award of all appropriate damages, including treble damages for the defendant's alleged

---

<sup>3</sup> Although not separately asserted, TecSec's infringement allegations also implicate independent claim 1 of the '702 patent, upon which claim 2 depends.

<sup>4</sup> Similarly, TecSec's allegations also implicate independent claims 7 and 10 of the '433 patent, upon which claims 8 and 12, respectively, depend.

willful infringement, and attorneys' fees and costs pursuant to 35 U.S.C. § 285. See Pl.'s Second Amend. Compl. at 98-99.

Defendant IBM is a New York corporation with its principal place of business in New York that manufactures and sells computer software and hardware. See id. ¶ 4. The IBM products accused of infringement in this civil action fall into three general categories: (i) IBM DB2 and IDS database products (accused of infringing the '702 patent family); (ii) IBM WebSphere and DataPower Appliance products (accused of infringing the '702 patent family and the '433 patent); and (iii) IBM System z mainframe server products (accused of infringing the '448 patent). See id. ¶¶ 31-33; 57-58; 82-83; 107-08; 132-33; 158-59. More specifically, the accused products include:

1. IBM's "database products": DB2 for z/OS; DB2 for LUW (Linux, UNIX, and Windows); and IDS (used in conjunction with Data Encryption Tool and Database Encryption Expert ("DEE")).
2. IBM's WebSphere products: WebSphere Application Server ("WAS"); WebSphere DataPower XML Security Gateway XS40; WebSphere DataPower Integration Appliance XI50; and WebSphere DataPower B2B Appliance XB60.
3. IBM's System z products: System z mainframe servers (z9 and z10) that incorporate Crypto Express2; and System z mainframe servers (z9 and z10) that incorporate Crypto Express3.

Id.

In its Motion for its Proposed Claim Constructions and Summary Judgment of No Infringement [Dkt. No. 462], IBM seeks summary judgment in its favor on all counts in plaintiff's Second Amended Complaint, arguing that TecSec has not come forward with sufficient evidence to establish a genuine material dispute regarding alleged

infringement of any of the six patents at issue. In its Motion for Partial Summary Judgment of Infringement [Dkt. No. 478], TecSec seeks judgment in its favor on claims 8 and 9 of the '702 patent and claim 4 of the '433 patent, along with several of the affirmative defenses raised by IBM in its First Amended Answer to TecSec's Second Amended Complaint.

## II. Standard of Review

Summary judgment is appropriate where the record demonstrates "that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). A genuine issue of material fact exists "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 247-48 (1986). The Court must view the record in the light most favorable to the nonmoving party. See Bryant v. Bell Atl. Md., Inc., 288 F.3d 124, 132 (4th Cir. 2002). However, the "mere existence of a scintilla of evidence in support of the [nonmovant's] position will be insufficient; there must be evidence on which the jury could reasonably find for the [nonmovant]." Anderson, 477 U.S. at 252; see also Othentec Ltd. v. Phelan, 526 F.3d 135, 140 (4th Cir. 2008).

Thus, if a nonmoving party bears the burden of proof on a claim at trial, the moving party may prevail on its Rule 56 motion by showing that there is a lack of evidence to carry the other party's burden as to any essential element of the cause of action.

See Celotex Corp. v. Catrett, 477 U.S. 317, 322-23 (1986); Cray Commc'ns Inc. v. Novatel Computer Sys., Inc., 33 F.3d 390, 393-94 (4th Cir. 1994). Once the moving party has met its burden of demonstrating the absence of an issue of material fact, the party opposing summary judgment may not rest on mere allegations or inferences, but must instead proffer specific facts or objective evidence showing that a genuine issue of material fact exists requiring further proceedings. Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 586 (1986).

### III. Discussion

#### **A. '702 (DCOM) Patent Family: Claim Construction**

In their cross-motions for summary judgment, the parties raised the issue of the proper construction of a number of terms in each of the patents in suit. The Court will construe only those terms that are strictly necessary to the resolution of the parties' motions. Specifically, in addressing the infringement claims for the '702 family of patents, the Court will construe the term "multi-level multimedia security," providing a construction for "multi-level . . . security" and "multimedia," in turn.<sup>5</sup>

##### 1. Legal standards for claim construction

The district court has the "power and obligation to construe as a matter of law the meaning of language used in the patent

---

<sup>5</sup> The Court will also construe the term "storing" in the '433 patent and the term "extract" in the '448 patent. See infra at III.C.1 & III.D.1. The legal standards set forth for claim construction, see infra at III.A.1, will apply equally to those constructions, as well.

claim." Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995), aff'd, 517 U.S. 370 (1996). As a starting point, a claim term is to be given the "ordinary and customary meaning" it would have had to a person of ordinary skill in the art at the time of the invention. Phillips v. AWH Corp., 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc); see also Dow Chemical Co. v. Sumitomo Chem. Co., Ltd., 257 F.3d 1364, 1372 (Fed. Cir. 2001). To determine that meaning, the court must first look to how the words of the claims themselves define the scope of the patented invention, and then look to "those sources available to the public that show what a person of skill in the art would have understood [the] disputed claim language to mean." Phillips, 415 F.3d at 1314; see also Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582-83 (Fed. Cir. 1996). The court must construe the entire claim, including any preamble, so long as it gives life and meaning to the invention claimed. See Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1305 (Fed. Cir. 1999).

For some claim terms, the ordinary meaning may be readily apparent, and construction of those terms therefore "involves little more than the application of the widely accepted meaning of commonly understood words." Phillips, 415 F.3d at 1314. If technical terms are used, the court may also "consult scientific dictionaries and technical treaties at any time" because "technical terms often have an 'ordinary meaning' as understood by one of skill in the art, although these same terms may not be readily familiar to a judge, or may be familiar only in a

different context." Dow Chemical, 257 F.3d at 1372. The meaning of a disputed claim term should be resolved primarily in light of the "intrinsic evidence of record, i.e., the patent itself, including the claims, its specification and, if in evidence, the prosecution history." Vitronics, 90 F.3d at 1582 (describing intrinsic evidence as "the most significant source of the legally operative meaning of disputed claim language"); see also Phillips, 415 F.3d at 1316 (holding that "[t]he construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction").

2. "Multi-level multimedia security" must be interpreted as a claim limitation in the '702 patent family.

The patents in the '702 family describe systems and methods for achieving "multi-level multimedia security" by means of a "distributed cryptographic object method" ("DCOM"). See, e.g., Def.'s Ex. 3 ('702 patent) at Abstract. Indeed, the phrase "multi-level multimedia security" appears in the preamble of each independent claim in the '702 (DCOM) patent family. See id. ("By effectuating compartmentalization of every object by label attributes and algorithm attributes, multi-level multimedia security is achieved."); see also Def.'s Ex. 4 ('755 patent) at Abstract (same); Def.'s Ex. 5 ('452 patent) at Abstract (same); Def.'s Ex. 6 ('781 patent) at Abstract (same). In the context of those patents, the phrase "multi-level multimedia security" is therefore a defining aspect of the invention, and it functions as



a crucial claim limitation.

"In considering whether a preamble limits a claim, the preamble is analyzed to ascertain whether it states a necessary and defining aspect of the invention, or is simply an introduction to the general field." On Demand Mach. Corp. v. Ingram Indus., Inc., 442 F.3d 1331, 1343 (Fed. Cir. 2006). In this case, "multi-level multimedia security" is not merely presented as relevant background information in the field; rather, all of the '702 (DCOM) patents stress the inventions' ability to provide multi-level and multimedia security as critical features of the claimed inventions. In fact, those words appear throughout the patents' specifications - in their Abstracts, their figures, the Field of the Invention, the Background of the Invention, the Summary of the Invention, the Detailed Description of the Invention, and the independent claims of the patents themselves. See Def.'s Exs. 3-6. Under these circumstances, the phrase "multi-level multimedia security" therefore must be regarded as a claim limitation. See Poly-Am., L.P. v. GSE Lining Tech., Inc., 383 F.3d 1303, 1310 (Fed. Cir. 2004); Gen. Elec. Co. v. Nintendo Co., 179 F.3d 1350, 1361-62 (Fed. Cir. 1999).

Moreover, the patentee expressly relied upon an explanation of "multi-level multimedia security" to distinguish prior art during prosecution of the DCOM patents, and TecSec has relied upon that phrase throughout the course of this litigation. See Def.'s Ex. 7 at IBMTS002635674 (patent prosecution history in which patentee distinguished the Preston patent because it allegedly

could not "cryptographically embed devices within other devices or within data files"); Def.'s Ex. 8 (demonstrating TecSec's reliance upon the '702 preamble to distinguish the prior art in response to IBM's Interrogatory No. 15); see also Br. in Supp. of Pl. TecSec's Mot. for Partial Summ. J. on Def.'s Affirmative Defenses of Invalidity and Inequitable Conduct [Dkt. No. 427] at 8 (arguing that the "embedding of encrypted objects within other objects creates the 'multi-level security' that is *essential* to the DCOM patents") (emphasis added). This further strengthens the Court's conclusion that the "multi-level multimedia security" phrase in the preamble of the '702 patent family must be read as a claim limitation. See, e.g., Computer Docking Station Corp. v. Dell, Inc., 519 F.3d 1366, 1375 (Fed. Cir. 2008); Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc., 289 F.3d 801, 808 (Fed. Cir. 2002).

3. "Multi-level . . . security" requires multiple layers of encryption.

IBM and TecSec offer different constructions of "multi-level . . . security," with IBM proposing a construction whereby "encrypted objects are nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption," while TecSec proffers the construction "security provided by the nesting of individually encrypted objects." Compare Def.'s Mot. for Summ. J. at 6 to Pl. TecSec's Br. in Opp. to IBM's Proposed Claim Constructions and Mot. for Summ. J. of No Infringement ["Pl.'s Br. in Opp."] at 6. The primary dispute between the parties concerns whether the

"container objects" - that is, the objects in which encrypted objects are nested - must necessarily be encrypted themselves. Under IBM's definition, the container objects must be encrypted, thereby resulting in multiple layers of encryption, while TecSec argues that the '702 patent "does not require the container object to be encrypted, but is broad enough to encompass implementations in which the container object may be encrypted." Id. (emphasis in original). For the reasons explained below, the Court will adopt IBM's construction.

a. IBM's construction is consistent with the intrinsic evidence.

IBM's proposed construction best conforms to the intrinsic evidence of record, including the patentee's own definition, as provided to the Patent and Trademark Office ("PTO"). For example, during prosecution of the '702 patent application, the PTO examiner rejected claim 1 - the only claim pending at that time - as indefinite under 35 U.S.C. § 112 ¶2 because it was "unclear what is meant by 'multi-level multimedia security.'" See Def.'s Ex. 7 at IBMTS002635653. To overcome the rejection, the patentee amended the application to "more clearly explain" the term. Id. at IBMTS002635672. Specifically, the patentee clarified that "[m]ulti-level security is achieved because encrypted objects may be nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption." Id. at IBMTS002635664; see also Ex. 3 ('702 patent) at 4:25-28 (same). The patentee then explained: "Thus, the nesting of

*individually encrypted objects* provides security that is multi-level and multimedia." Def.'s Ex. 7 at IBMTS002635664.

It is well established that "[t]he patentee is free to act as his own lexicographer, and may set forth any special definitions of the claim terms in the patent specification or file history, either expressly or impliedly." Schoenhaus v. Genesco, Inc., 440 F.3d 1354, 1358 (Fed. Cir. 2006); see also Irdeto Access, Inc. v. Echostar Satellite Corp., 383 F.3d 1295, 1300 (Fed. Cir. 2004); Home Diagnostics, Inc. v. LifeScan, Inc., 381 F.3d 1352, 1356 (Fed. Cir. 2004). The patentee's definition of "multi-level . . . security" during patent prosecution is therefore binding as a matter of law. See Honeywell, Inc. v. Victor Co. of Japan, Ltd., 298 F.3d 1317, 1323-24 (Fed. Cir. 2002); CVI/Beta Ventures, Inc. v. Tura LP, 112 F.3d 1146, 1158 (Fed. Cir. 1997); see also Medrad, Inc. v. MRI Devices Corp., 401 F.3d 1313, 1318 (Fed. Cir. 2005) ("A patentee may define a particular term in a particular way, and in that event the term will be defined in that fashion for purposes of that particular patent, no matter what its meaning in other contexts.") (citation omitted).

Moreover, despite the somewhat confusing use of the phrase "may be nested," the '702 patentee's definition, read as a whole, makes clear that the claimed functionality of the '702 (DCOM) invention is a method of "multi-level" encryption in which encrypted objects are necessarily embedded or nested within other encrypted "container" objects, thereby "resulting in multiple layers of encryption." See Def.'s Ex. 7 at IBMTS002635664

(emphasis added). Indeed, the patentee further represented to the examiner that "[c]ontainer objects can only be 'opened' by users having access authority in the form of a cryptographic key," thereby clearly conveying that the container objects were themselves meant to be securely encrypted such that only authorized users could access them. See Def.'s Ex. 7 at IBMTS002635673. Given this context, the phrase "may be nested" must be interpreted to mean that encrypted objects are "capable of being nested" within other encrypted objects. Such nesting is not optional; rather, it is the essence of the claimed invention.<sup>6</sup> To find otherwise would read out of the DCOM patents the required "multiple layers of encryption" cited to the examiner.

b. TecSec's definition is inconsistent with the evidence and must be rejected.

TecSec's proposed construction is inconsistent with the patentee's definition of the patent's capabilities and therefore must be rejected. In particular, TecSec's interpretation would impermissibly broaden the '702 patent, reading it to cover not only situations in which encrypted objects are nested within other

---

<sup>6</sup> Indeed, the patentee's definition of "multi-level security" in the '702 patent is part of a larger paragraph that describes the required capabilities of the invention. See Def.'s Ex. 3 at 4:14-34 ("The present invention is able to increase the security . . . [and] has the capability to embed objects . . . [and] allows users to distribute multiple encrypted objects . . . [which] may be nested within other objects which are also encrypted . . . resulting in multiple layers of encryption."). Nothing in the definition suggests that these capabilities are optional; rather, they are required to distinguish the invention from the prior art and to provide sufficient definiteness to overcome the PTO examiner's initial rejection. See Def.'s Ex. 7 at IBMTS002635653; id. at IBMTS002635664.

encrypted objects, thereby providing multi-layer encryption, but also situations in which the container objects are not encrypted, which would necessarily result in only a single level of encryption. Accordingly, TecSec's contention that a patent directed at "multi-level security" requires only a single layer of encryption flatly contradicts the plain language of the claims, as well as the patentee's binding statements during patent prosecution. TecSec's construction must be rejected for those reasons alone. See Haemonetics Corp. v. Baxter Healthcare Corp., 607 F.3d 776, 782 (Fed. Cir. 2010).

TecSec's proposed definition is also inconsistent with the '702 patent specification, which repeatedly and consistently describes the claimed invention as one in which objects are encrypted and then nested or embedded within other encrypted objects. For example, in the "Summary of the Invention" section, the patent explains that one of the objectives of the invention is to allow for the embedding of objects within other objects, "resulting in an access hierarchy for users of the system." Def.'s Ex. 3 at 3:21-24. The patent further explains that once encrypted objects are embedded within container objects, those container objects are also encrypted. See id. at 5:32-41.<sup>7</sup> In fact, each and

---

<sup>7</sup> TecSec attempts to avoid the conclusion that the container object must itself be encrypted by arguing that the patent's definition of a container object as "an object that contains other objects, [which] can be either cipher text or plain text," see Def.'s Ex. 3 at 5:3-5, means that container objects need not be encrypted. That definition, however, states

every example of the invention identified in the '702 patent specification describes multiple layers of encryption capability, and every figure depicting the invention shows one or more encrypted objects embedded within other encrypted objects. See, e.g., id. at 7:50-58 (describing examples of multi-layered encryption); Fig. 3 (showing rings of concentric circles in which encrypted objects are embedded in other encrypted objects); 11:18-30 (describing Figure 3); see also id. at Fig. 4; 4:47-49 (describing Fig. 4 as "an encrypted object that contains a web of embedded encrypted objects nested within it"). As a result, IBM's definition, under which at least one encrypted object must be embedded within another encrypted object, is the only construction that faithfully adheres to the patentee's own descriptions of the claimed invention. See Phillips, 415 F.3d at 1316 ("Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim.").

c. IBM's construction does not violate the doctrine of claim differentiation.

Finally, TecSec argues that IBM's proposed construction duplicates the language of claim 4 in the '702 patent and thereby violates the principles of claim differentiation. The doctrine of

---

only that the objects *within* the "container object" can be either cipher text or plain text; it plainly does not state that the container object itself need not be encrypted. Indeed, as explained above, every example and figure in the '702 patent shows that the container objects are encrypted.

claim differentiation "presumes that there is a difference in scope among the claims of a patent," and therefore requires a court to interpret the patent such that each independent claim carries its own unique meaning. Multi-form Desiccants, Inc. v. Medzam, Ltd., 133 F.3d 1473, 1479 (Fed. Cir. 1998). TecSec contends that IBM's proposed definition violates that doctrine because it would read into claims 1 and 2 of the '702 limitations that are separately added in claim 4, such as the requirement in claim 4 that a "second object" be encrypted and labeled with a "second object label."

However, TecSec's claim differentiation argument has no basis in the law or in a logical reading of the '702 patent's claims. Specifically, independent claim 1 of the '702 patent claims "[a] method for providing multi-level multimedia security in a data network," comprising nine different steps. See Def.'s Ex. 3 at 12:2-16. Dependent claim 2, which is asserted in this action, claims "[t]he method of claim 1, wherein the object is an application document, and further comprising" two additional steps. Id. at 12:17-19. Finally, dependent claim 4, which is also asserted in this action, describes:

The method of claim 3 [which itself depends on independent claim 1], further comprising the steps of:

- (A) selecting a second label for the second object;
- (B) selecting an encryption algorithm;
- (C) encrypting the second object; and
- (D) labelling [sic] the second encrypted object with a second object label."



Id. at 12:27-33 (emphasis added). TecSec uses the "second object" language in claim 4 to argue that "multi-level multimedia security" cannot mean that two objects need to be nested and encrypted, thereby resulting in multi-layered encryption, because then claim 4 would have no independent meaning.

However, as described above, the term "multi-level . . . security" is a separate element of the '702 patent and must be read as imposing an additional limitation beyond the other language in the claims (including claim 4), because the patent "must be interpreted with an eye toward giving effect to all terms in the claim." Becton, Dickinson & Co v. Tyco Healthcare Group, LP, 616 F.3d 1249, 1257 (Fed. Cir. 2010) (citation omitted). Furthermore, TecSec's claim differentiation argument fails because "the claims are not rendered identical" by the construction. Sinorgchem Co., Shandong v. Int'l Trade Comm'n, 511 F.3d 1132, 1140 (Fed. Cir. 2007) (emphasis added). Specifically, as cited above, claim 4 in the '702 patent requires steps beyond simply embedding and encrypting a second object, including "selecting a second label" and "labelling [sic] the second encrypted object" with that additional label. See Def.'s Ex. 3 at 12:29-33. Claim differentiation is therefore inapplicable in this instance.

Moreover, in this case, where the patentee explained the meaning of a term during prosecution to obtain allowance of a claim, claim differentiation simply cannot be used to change the meaning of that term. In Andersen Corp. v. Fiber Composites, LLC, 474 F.3d

1361 (Fed. Cir. 2007), the Federal Circuit made clear that "the written description and prosecution history [of a patent] overcome any presumption arising from the doctrine of claim differentiation." Id. at 1370 (citing Kraft Foods, Inc. v. Int'l Trading Co., 203 F.3d 1362, 1368 (Fed. Cir. 2000)). Indeed, "the doctrine of claim differentiation cannot broaden claims beyond their correct scope, determined in light of the specification and the prosecution history." Multi-form Desiccants, 133 F.3d at 1480. As such, "claims that are written in different words may ultimately cover substantially the same subject matter." Id. This is just such a case, and TecSec's claim differentiation argument therefore cannot overcome the explicit definition provided by the patentee.

For all these reasons, the Court will construe the term "multi-level . . . security" to mean "security achieved when encrypted objects are nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption." Under that construction, at least one encrypted object *must* be nested within at least one other encrypted object, thereby achieving multi-level, multi-layer security.

#### 4. Construction of "multimedia"

IBM also seeks construction of the word "multimedia" in the "multi-level multimedia security" claim limitation of the '702 patent, proposing the definition: "a computer technology that displays information using a combination of full-motion video, animation, sound, graphics, and text with a high degree of user

interaction." See Def.'s Mot. for Summ. J. at 6. TecSec has not specifically offered a competing construction of "multimedia," but instead argues that multimedia security can encompass the encryption of many different types of objects, and that "multi-level multimedia security" should be defined merely as "security provided by the nesting of individually encrypted objects." See Pl.'s Br. in Opp. at 6-9.

TecSec's interpretation of "multimedia security," however, does not square with the intrinsic evidence and prosecution history, nor does it reflect the plain meaning of the term to a person of ordinary skill in the art at the time of the invention. Rather, TecSec's proposed construction of "multi-level multimedia security" would read "multimedia" out of the claims entirely, and would improperly expand the '702 patent's scope to capturing situations in which objects of only a single type of medium are encrypted - the exact opposite of multimedia security. TecSec's efforts to ignore the additional claim limitation imposed by the patentee's repeated use of the word "multimedia" in the '702 patent must therefore be rejected. See Tex. Instruments Inc. v. U.S. Int'l Trade Comm'n, 988 F.2d 1165, 1171 (Fed. Cir. 1993) ("[T]o construe the claims in the manner suggested by [the plaintiff] would read an express limitation out of the claims. This we will not do.").

Moreover, the applicant for the '702 patent also explicitly defined "multimedia" by amending the application and providing a technical dictionary definition to overcome an indefiniteness

rejection by the PTO examiner. Specifically, the applicant amended the patent to explain that the "invention encrypts any object, encompassing all forms of media," see Def.'s Ex. 7 at IBMTS002635664, and then directed the patent examiner to a definition of "multimedia" in Peter Dyson's The PC User's Essential Accessible Pocket Dictionary (hereinafter "Dyson dictionary"), which defines "multimedia" as "[a] computer technology that displays information using a combination of full-motion video, animation, sound, graphics, and text with a high degree of user interaction." Id.; see also Def.'s Ex. 10 at 354 (Dyson dictionary definition). The patentee's unambiguous reliance on that dictionary definition of "multimedia" is therefore "binding in litigation" as a matter of law. CVI/Beta Ventures, 112 F.3d at 1158. Accordingly, the Court will adopt IBM's construction of "multimedia" and will construe that term to mean "a computer technology that displays information using a combination of full-motion video, animation, sound, graphics, and text with a high degree of user interaction."

#### B. '702 (DCOM) Patent Family: Infringement Allegations

"A patentee claiming infringement must present proof that the accused product[s] meet[] each and every claim limitation." Forest Labs, Inc. v. Abbott Labs, 239 F.3d 1305, 1310 (Fed. Cir. 2001). The patentee must also prove that the accused infringer either directly infringes the patent under 35 U.S.C. § 271(a), by "mak[ing], us[ing], offer[ing] to sell, . . . sell[ing], . . . or import[ing]" the patented invention, or indirectly infringes the

patent under 35 U.S.C. § 271(b) or § 271(c), by "actively induc[ing]" infringement or by contributing to infringement.

Failure to provide the proof necessary to establish a genuine issue of material fact on those points warrants summary judgment of no infringement. See Celotex, 477 U.S. at 325.

Throughout its Motion for Summary Judgment, IBM successfully demonstrates that despite extensive discovery, TecSec has failed to identify any actual instance of infringement by either IBM or any of its customers. Mere speculation is insufficient to allow a case to proceed to trial; accordingly, none of TecSec's many theories of infringement can survive summary judgment.

1. Plaintiff's theory of direct infringement

TecSec first accuses IBM of directly infringing each asserted claim of the '702 patent family, including both the method claims and the system claims.<sup>8</sup> However, those allegations fail as a matter of law because TecSec has produced no evidence that IBM itself ever performed every claimed step of the asserted method claims, or ever made, used, sold, or offered to sell the entire claimed systems.

To establish direct infringement, the patentee must prove that the alleged infringer either made, used, offered to sell, or sold in the United States, or imported into the United States, the patented

---

<sup>8</sup> Claim 2 of the '702 patent is a method claim, as are claims 1, 2, 3, 10, and 13 of the '781 patent, and all of the asserted claims of the '755 patent and the '452 patent (claims 1 and 2 of the '755 patent, and claims 1, 2, and 13 of the '452 patent, respectively). The remaining claims (claims 8, 9, 12, 14, and 15 of the '702 patent, and claims 14 and 15 of the '781 patent) are system claims.

invention. See 35 U.S.C. § 271(a). "Direct infringement . . . is limited to those who practice each and every element of the claimed invention." BMC Res., Inc. v. Paymentech, L.P., 498 F.3d 1373, 1381 (Fed. Cir. 2007). Accordingly, the Federal Circuit has held that "liability for [direct] infringement requires a party to make, use, sell, or offer to sell the patented invention, meaning the entire patented invention." Id. at 1380 (emphasis added). As a result, a party that makes, uses, sells, offers to sell, or imports less than the entire patented invention is not a direct infringer as a matter of law. See Rotec Indus., Inc. v. Mitsubishi Corp., 215 F.3d 1246, 1252 n.2 (Fed. Cir. 2000) (holding that "one may not be held liable under § 271(a) for making or selling less than a complete invention").

#### a. Method claims

To show that IBM directly infringed the asserted method claims, TecSec must establish that IBM either used or performed every step of the claimed methods. See Joy Techs., Inc. v. Flakt, Inc., 6 F.3d 770, 775 (Fed. Cir. 1993) ("A method claim is directly infringed only by one practicing the patented method.") (emphasis omitted); see also BMC Res., 498 F.3d at 1381. However, TecSec has utterly failed to come forward with any evidence that IBM itself performed any of the steps of the method claims.

Indeed, TecSec effectively conceded in its briefing that IBM's products do not directly infringe the asserted method claims in the '702 patent family. For example, in response to IBM's Motion for

Summary Judgment, in which defendant argued that its database products do not directly infringe the '702 family of patents, TecSec contended only that "IBM has made, sold, and offered for sale the accused IBM database [DB2 and IDS] products, which infringe each of the asserted claims of the '702 patent family." See Pl.'s Br. in Opp. at 2 (responding to IBM's Statement of Fact No. 2). Notably missing from TecSec's response, however, is any allegation that IBM itself "used" the patented method in its database products. See id. Moreover, TecSec has also failed to come forward with any evidence creating a genuine dispute of material fact that IBM performs every step of the asserted method claims with any of the accused Websphere products. It is axiomatic that there can be no direct infringement by IBM of any method claim absent IBM's own use or performance of each and every step of that method. See Joy Techs., 6 F.3d at 775. Accordingly, summary judgment is appropriate in IBM's favor on plaintiff's allegations of direct infringement of the asserted method claims in the '702 (DCOM) patents.

#### b. System claims

TecSec's direct infringement allegations for the system claims in the '702 patent family also fail as a matter of law. To prove that IBM directly infringed the system claims, plaintiff must show that IBM made, used, sold, offered for sale, or imported the entire claimed system(s). See Rotec, 215 F.3d at 1252 n.2; BMC Res., 498 F.3d at 1380. However, TecSec has failed to come forth with any evidence that IBM has actually done so. Instead, TecSec simply

accuses various types of IBM software of infringement. That software, of course, constitutes at most only part of the claimed systems, as the software must be installed on a computer and combined with hardware to infringe. Indeed, TecSec's infringement theories for the system claims, all of which involve hardware such as a "system memory means for storing data," require that the accused products be "installed, as intended, in computers comprising digital logic means." See Br. in Supp. of Pl. TecSec's Mot. for Partial Summ. J. of Infringement at 18. As a matter of law, making or selling software without the claimed hardware does not constitute direct infringement of a system claim, and summary judgment is therefore appropriate in favor of IBM on those claims, as well. See Rotec, 215 F.3d at 1252 n.2.

Moreover, throughout discovery, TecSec struggled to identify how IBM's accused products allegedly infringe the '702 patent family. Plaintiff ultimately relied on very specific accused "scenarios," involving particular combinations and configurations of products. Indeed, during discovery, TecSec and its experts offered six different "infringing cases" under which IBM's database products, for example, purportedly infringe the asserted claims of the '702 patent family. Those six infringing cases can be summarized roughly as follows:

1. DB2 for z/OS (versions 8+) used in combination with the IBM Data Encryption for IMS and DB2 Databases tool ("Data Encryption Tool"), where the claimed encrypted "object" is a column within a table in a DB2 database;
2. DB2 for z/OS (versions 8+) using the built-in "column-level encryption," where the claimed "object" is a column within a table in a DB2 database;



3. DB2 for LUW (versions 9.1+) using the built-in "column-level encryption," where the claimed "object" is a column within a table in a DB2 database;
4. DB2 for LUW (versions 8.2+ with FixPack 14) using the IBM Database Encryption Expert ("DEE"), where the claimed object is non-meta data file contents of the DB2 database tablespace;
5. IDS (versions 10+) using the built-in "column-level encryption" applied to the data within a column in a table in an IDS database; and
6. IDS (versions 11+) with an instance of DEE (at least version 1.1 with FixPack 3 for IDS version 11.X support), allowing for encryption of the non-meta data portions of a tablespace of an IDS database.

See Def.'s Ex. 16 (TecSec's interrogatory responses and infringement charts explaining the alleged infringement scenarios).

For each of those accused "scenarios" of IBM's database products to constitute infringement, highly specific hardware and other configuration requirements must be met. For example, certain infringing cases specify the exact IBM hardware computers on which the software and operating systems must be installed, along with additional hardware elements that may be required. See, e.g., id. at Ex. 1 at 1 (Infringing Case 1, requiring "one of the following IBM hardware computers: z800, z900, z890, z990, z9 and z10" and indicating that "crypto co-processor[s] (e.g., Crypto Express2 or Crypto Express3)" may be required; see also id. at Ex. 1 at 2 (Infringing Case 3, indicating that the required hardware elements can include, inter alia, a 64-bit Common Hardware Reference Platform (CHRP) architecture; Itanium-based HP Integrity Series systems (IA-64), PA-RISC (PA-8x00)-based HP 900 Series 700 and Series 800 systems; z86 (Intel Pentium 4 or higher, Intel Xeon and AMD Athlon),

x86-64 (Intel EM64T and AMD64), IA64 (Intel Itanium 2 or higher), POWER® (IBM eServer OpenPower, iSeries or pSeries systems that support Linux, [or] eServer System z or System z9). Other scenarios require various functions to be enabled within the accused system before the asserted systems in the '702 (DCOM) patents are infringed. See, e.g., id. at Ex. 1 at 1 (Infringing Case 2, requiring that "[i]f RACF is used, then RACF must be enabled in the z/OS operating system. In addition, to perform encryption, the system must have Integrated Cryptographic Service Facility (ICSF) enabled within z/OS.").

Similarly, TecSec cannot dispute that a single DataPower or Websphere Application Server ("WAS") product, standing alone, cannot infringe the '702 patent family, because, among other reasons, those products alone are not capable of encrypting and decrypting the same object, as is required by the '702 (DCOM) patents. See infra at III.B.3.c. Instead, TecSec asserts that a combination of IBM products infringe the '702 patents because IBM and its customers can use and implement a WAS-WAS or WAS-DataPower configuration of products to perform the claimed encryption and decryption of the same "object." See Pl.'s Br. in Opp. at 16-17 (describing how IBM's products can be "set up," combined, and implemented to infringe). Accordingly, a user must first configure IBM's WAS software to communicate with other WAS or DataPower software before it can even potentially infringe.

TecSec's speculative theories of infringement fail because plaintiff has not submitted any evidence that IBM actually makes,

sells, offers for sale, or imports an entire infringing database system, as described and configured according to the very precise specifications offered by plaintiff's experts in their "infringing cases." Nor does TecSec cite any actual evidence that IBM makes, sells, offers for sale, or imports the specific WebSphere product combinations that TecSec alleges infringe. In fact, TecSec's theory appears to reduce to the contention that IBM's users or customers may theoretically be able to install IBM software onto a computer system and then combine and configure it into one of the accused scenarios. See, e.g., Def.'s Ex. 17 (Stubblebine Expert Report) at 15 ("At a user's direction, any one of four different access control techniques is implemented by DB2, z/OS, or the [Data Encryption] Tool."). However, even if some user-implemented system were to meet all of the asserted claim limitations - which, as explained below, it cannot, see infra at III.B.3, - TecSec has provided no evidence that IBM ever made, used, sold, offered to sell, or imported that entire claimed system, and TecSec's direct infringement claims therefore fail as a matter of law. See Rotec, 215 F.3d at 1252 n.2; see also Centillion Data Sys., LLC v. Owest Commc'ns Int'l, Inc., - F.3d -, 2011 WL 167036, at \*6-\*7 (Fed. Cir. Jan. 20, 2011) (finding that "[s]upplying the software for the customer to use is not the same as using the system" and that, as a matter of law, the defendant did not "make" the accused system because "[t]he customer, not [the defendant], completes the system and . . . install[s] the client software").

## 2. Plaintiff's theories of indirect infringement

TecSec also accuses IBM of indirect infringement, based upon the sales of its database and WebSphere products to its customers. "When a defendant participates in or encourages infringement but does not directly infringe a patent, the normal recourse under the law is for the court to apply the standard for liability under indirect infringement." BMC Res., 498 F.3d at 1379. Indirect infringement may be proven by evidence of "inducing infringement" or "contributory infringement." 35 U.S.C. §§ 271(b) & (c).

To establish induced infringement, a patentee must prove that the defendant "actively induce[d] infringement of a patent." 35 U.S.C. § 271(b). As a required predicate, the patentee must establish that some other third party committed the entire act of direct infringement. See BMC Res., 498 F.3d at 1380. Additionally, the patentee must show that the alleged infringer took specific acts to knowingly induce the infringement. In fact, as the Federal Circuit has held, "[t]he plaintiff has the burden of showing that the alleged infringer's actions induced infringing acts and that he knew or should have known his actions would induce actual infringements." DSU Med. Corp. v. JMS Co., 471 F.3d 1293, 1304 (Fed. Cir. 2006) (en banc) (citations and quotations omitted).

To establish contributory infringement, a patentee must show that the alleged infringer offered to sell or sold a component of a patented apparatus that constitutes a material part of the invention, with knowledge that the component is especially made or adapted for use in an infringement and is not a staple article

suitable for substantial non-infringing use. See 35 U.S.C. § 271(c). As with inducing infringement, contributory infringement requires proof of a mens rea of at least knowledge, and also requires, as a predicate, that some other party committed the entire act of direct infringement. See BMC Res., 498 F.3d at 1379, 1381.

a. TecSec produced no evidence of direct infringement by any third party.

In this case, even after extensive discovery - comprising over 7 million pages of documents, 40 depositions, and 55 subpoenas to IBM's customers - TecSec has failed to present even a single instance of a customer using the accused IBM products in an allegedly infringing manner. As the plaintiff in this case, TecSec bears the "burden to show direct infringement for each instance of indirect infringement," DSU Med., 471 F.3d at 1301, and the Federal Circuit has held that "it is not enough to simply show that a product is capable of infringement; the patent owner must show evidence of *specific instances* of direct infringement" by a third party. Fujitsu Ltd. v. Netgear Inc., 620 F.3d 1321, 1329 (Fed. Cir. 2010) (emphasis added); see also ACCO Brands, Inc. v. ABA Locks Mfr. Co., 501 F.3d 1307, 1313 (Fed. Cir. 2007) ("In order to prove direct infringement, a patentee must either point to specific instances of direct infringement or show that the accused device necessarily infringes the patent in suit.").

TecSec has simply failed to meet that burden. During discovery, IBM expressly asked TecSec to provide "an identification of each person that TecSec contends directly infringed" the asserted DCOM patent claims; TecSec provided no response. See

Def.'s Ex. 11 at 13-15. Nor has TecSec's expert identified any such direct infringer. Moreover, at oral argument on the instant motions, TecSec's counsel pointed to a list of IBM customers, such as Kroger, who have purchased the accused IBM products, claiming that they might infringe the DCOM patents. However, those customers have all responded to plaintiff's subpoenas denying that they use the products in the allegedly infringing manner, see, e.g., IBM's Reply Br. in Supp. of its Proposed Claim Constructions and Mot. for Summ. J. of No Infringement ["Def.'s Reply Br."] at Ex. 45 (Kroger's response to TecSec's subpoena), and TecSec has produced no evidence contradicting those denials. TecSec's failure to uncover evidence of even a single third-party direct infringer is fatal to its indirect infringement claims. See E-Pass Techs. v. 3COM Corp., 473 F.3d 1213, 1222-23 (Fed. Cir. 2007) ("If, as [plaintiff] argues, it is 'unfathomable' that no user in possession of one of the accused devices . . . has practiced the accused method . . . [plaintiff] should have had no difficulty in meeting its burden of proof and in introducing testimony of even one such user.").

TecSec attempts to cure the deficiencies in its direct proof with circumstantial evidence, alleging that IBM instructs its customers to use the products in an infringing manner in various advertising, testimonial, and other "puff piece" materials, and that IBM's customers must be using the products to infringe because the patented features are required to ensure regulatory compliance with various security and encryption standards. See, e.g., Pl.'s

Br. in Opp. at 15-16. However, TecSec's circumstantial evidence is equally unpersuasive, as TecSec has identified nothing in IBM's advertising materials teaching all of the claimed steps or elements in combination. In fact, TecSec has not cited a single document in which IBM instructs its customers to implement the exact scenarios that TecSec contends infringe the '702 patent family, all of which require a specific combination and configuration of products, supported by particular hardware and other specified elements, before they are even capable of infringing. Accordingly, "it requires too speculative a leap to conclude that any customer actually performed the claimed method." E-Pass, 473 F.3d at 1222.

Moreover, TecSec has not provided any evidence specifically connecting the patented inventions to any regulatory requirements with which IBM or its customers must comply, such as the Payment Card Industry (PCI) standard, Sarbanes-Oxley, HIPAA, or state data breach laws. In support of its contentions, TecSec relies upon the "expert" opinion of Sajay Rai, but his opinion is without foundation and therefore must be disregarded, as he admitted never seeing the patents in suit, let alone comparing any of the asserted claims in those patents to any regulatory requirements. See Def.'s Reply Br. at Ex. 46 (Rai Deposition) at 75:9-18 ("Q: Have you actually seen any of the patents in this case? A: No. . . . I have no knowledge of the patents."). TecSec's claim that IBM customers use the allegedly infringing features to achieve regulatory compliance is therefore pure speculation unsupported by any admissible evidence. Indeed, Rai could not identify a single IBM

customer who allegedly used the patented methods or systems during his deposition, see id. at 214:10-217:6, and his purported opinion is directly contrary to the 55 subpoenas served by TecSec on IBM's customers that failed to yield evidence of even a single instance of such infringement.

Finally, TecSec's attempt to rely upon circumstantial evidence fails as a matter of law because TecSec cannot show that the accused products necessarily infringe the asserted patents. See Exergen Corp. v. Wal-Mart Stores, Inc., 575 F.3d 1312, 1322 (Fed. Cir. 2009) ("Because [plaintiff] submitted no evidence of any specific instance of direct infringement, [plaintiff] was required to show that the accused device necessarily infringes the patent in suit.") (internal citations and quotations omitted); see also ACCO Brands, 501 F.3d at 1313. Indeed, the undisputed record evidence shows that the accused products can be, and in fact are intended to be, used in a variety of different ways that do not infringe, even under TecSec's own theories. For example, IBM's customers can use access control without encrypting, and vice versa; meanwhile, the accused database products do not need to be configured in the very specific ways outlined in TecSec's chart of alleged infringing cases. TecSec's "circumstantial evidence" theory therefore fails as a matter of law, and summary judgment is appropriate in favor of the defendant. Exergen, 575 F.3d at 1322.

b. TecSec produced no evidence of induced infringement by IBM.

Even if TecSec could somehow show direct infringement by a third party of any of the asserted '702 patent family claims, it



has not identified sufficient evidence that IBM actively induced such infringement, as required by 35 U.S.C. § 271(b). See ACCO Brands, 501 F.3d at 1213; DSU Med., 471 F.3d at 1304. Indeed, TecSec cites no evidence that IBM knew or should have known that its actions would induce actual infringement, and in response to IBM's interrogatory seeking plaintiff's bases for its claims that IBM induced third-party infringement, TecSec identified nothing to support a finding of the requisite mens rea of knowledge or intent.<sup>9</sup> See Def.'s Ex. 11 at 13-14. Instead, TecSec merely referenced its infringement contentions and expert reports, neither of which contains any evidence that IBM intended to cause infringement, or that it took actions knowing that those actions would result in infringement by third parties.

In fact, TecSec's inducement allegations are further weakened by its failure to identify any evidence that IBM even had knowledge that certain configurations or uses of its products might infringe the specific methods taught in the asserted patents. See Dynamis, Inc. v. Leepoxy Plastics, Inc., 831 F. Supp. 651, 655 (N.D. Ind. 1993) (finding that proof that defendants saw certain patent numbers is insufficient to support a contention that "the defendants knew that a method . . . was subject to a patent which

---

<sup>9</sup> In Global-Tech Appliances, Inc. v. SEB S.A., No. 10-6, the Supreme Court will address whether the legal standard for the "state of mind" element of a claim for actively inducing infringement under 35 U.S.C. § 271(b) is "deliberate indifference of a known risk" that an infringement may occur or instead "purposeful, culpable expression and conduct" with the specific intent of encouraging such an infringement. Under either standard, however, TecSec has failed to present sufficient evidence of induced infringement.

[defendant's] customers would infringe by using [defendant's] product"). Moreover, as with its other theories of infringement, TecSec is unable to point to any evidence that IBM ever encouraged its customers to implement any of the specific configurations or uses that allegedly infringe. Undisputed evidence cited by the plaintiff itself in fact demonstrates the exact opposite: that IBM recommended against using the products in the allegedly infringing manner. See, e.g., Buroker Decl., Ex. 51 at 5 ("The use of the encrypt and decrypt built-in column functions are not recommended"); see also Ex. 47 at 271:12-16 ("Not only have I not recommended it. I typically recommend against it.").

On this record, there is no evidence that IBM had the required intent to actively induce or cause infringement, and as a matter of law, summary judgment of no induced infringement is appropriate. See Vita-Mix Corp. v. Basic Holding, Inc., 581 F.3d 1317, 1329 (Fed. Cir. 2009) (affirming a grant of summary judgment of no inducement where instructions teaching non-infringing uses evidenced intent to discourage infringement and could not support any inference of intent to encourage infringement); see also Warner-Lambert Co. v. Apotex Corp., 316 F.3d 1348, 1365 (Fed. Cir. 2003) (affirming summary judgment of no inducement because "[e]specially where a product has substantial noninfringing uses, intent to induce infringement cannot be inferred even when the defendant has actual knowledge that some users of its product may

be infringing the patent").<sup>10</sup>

c. TecSec presented no proof of contributory infringement by IBM.

TecSec also failed to present evidence that IBM contributed to any third party's infringement of the '702 family of patents. Indeed, in response to IBM's interrogatory seeking TecSec's support for its claims of contributory infringement under 35 U.S.C. § 271(c), TecSec again merely referenced its infringement contentions and expert reports, which are devoid of any such supporting evidence. See Def.'s Ex. 11 at 14-15. Moreover, as explained above, there is no genuine dispute that the accused products can be used in many different ways that do not infringe the '702 (DCOM) patents, even under TecSec's theories, and TecSec has proffered no evidence to the contrary. Nor has plaintiff come forward with any evidence that IBM had the required knowledge "that the combination for which its components were [allegedly] especially made was both patented and infringing." Golden Blount, Inc. v. Robert H. Peterson Co., 365 F.3d 1054, 1061 (Fed. Cir. 2004) (internal citations and quotations omitted).

Instead, TecSec simply asserts that "to the extent that the accused IBM software is found to be a component of a patented machine or process, TecSec can demonstrate contributory

---

<sup>10</sup> This case is therefore distinguishable from Lucent Techs., Inc. v. Gateway, Inc., 580 F.3d 1301 (Fed. Cir. 2009), upon which plaintiff relies. In Lucent, the defendant's instructions clearly encouraged using the accused functionalities to infringe the asserted claim. Id. at 1323. Moreover, unlike here, there was no evidence in Lucent that the defendant specifically recommended against using the accused functions.

infringement because IBM sells its software knowing that when it is installed on a system, it will operate in an infringing manner." See Pl.'s Br. in Opp. at 29. However, plaintiff cannot avoid summary judgment now simply by responding that it may be able to prove its claim later. See Berckelely Inv. Group, Ltd. v. Colkitt, 455 F.3d 195, 201 (3d Cir. 2006) ("[S]ummary judgment is essentially 'put up or shut up' time for the non-moving party: the non-moving party must rebut the motion with facts in the record and cannot rest solely on assertions made in the pleadings, legal memoranda, or oral argument."). Accordingly, because TecSec has failed to present any evidence supporting a contributory infringement claim under 35 U.S.C. § 271(c), summary judgment must be entered for IBM.

3. The accused products do not meet all of the required claim limitations of the '702 patent family.

In addition to TecSec's failure to produce any evidence supporting its allegations of direct or indirect infringement of the '702 (DCOM) patent family, plaintiff's allegations are untenable as a matter of law because there is no genuine dispute that IBM's accused products do not meet all of the required claim limitations of the DCOM patents, either alone or in combination. See Exigent Tech., Inc. v. Atrana Solutions, Inc., 442 F.3d 1301, 1309 (Fed. Cir. 2006) ("[N]othing more is required than the filing of a summary judgment motion stating that the patentee had no evidence of infringement and pointing to the specific ways in which accused systems did not meet the claim limitations.").

a. The accused database products do not provide "multi-level multimedia security."

As discussed above, the claims of the '702 patent family require a system or method for providing "multi-level multimedia security" in a data network, such that "encrypted objects are nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption." See supra at III.A.2-4; see also Def.'s Exs. 3-6 ('702 family of patents). But on the record before the Court, there is no genuine dispute that none of the accused IBM products infringes those claims; indeed, at most, each provides only a single layer of encryption.<sup>11</sup>

Indeed, with respect to IBM's database products, TecSec has identified no actual evidence that any of the accused scenarios is even capable of providing multiple layers of encryption. Plaintiff's infringement chart identifies only one allegedly encrypted "object" for each given infringing case (e.g., "a table," "a column within a table," "non-meta data file content," or "non-meta data portions of a tablespace"), see Def.'s Ex. 16, and TecSec has not provided an explanation as to how each accused scenario itself could achieve the claimed "multi-level security," which

---

<sup>11</sup> TecSec cites certain documents using the phrase "multi-level security," which it claims refers to the capability of providing the layered and nested encryption claimed in the '702 family of patents. However, that phrase, as used in the cited IBM documents, is entirely unrelated to encryption. Rather, it appears to refer to mechanisms for protecting information by identifying users and access privileges based upon the DOD "Orange Book" published in 1983 - nearly a decade before TecSec applied for the '702 patent. See Clark Decl. [Dkt. No. 467] ¶ 25.

requires "encrypted objects [that] are nested within other objects which are also encrypted," see supra at III.A.3.<sup>12</sup> Moreover, during the discovery phase of this litigation, TecSec was ordered to identify exactly where in IBM's source code each and every claim limitation is found. See Dkt. No. 364 (Sept. 24, 2010 Order of Magistrate Judge Buchanan). In response, TecSec provided no source code citation for the "multi-level security" element. See Def.'s Ex. 16 at Ex. 1.

In its Opposition to IBM's Motion for Summary Judgment, TecSec does not explicitly dispute that none of the six accused "scenarios" includes multiple levels of encryption. Rather, for the first time in its brief, TecSec points to two alternative product combinations that allegedly provide "multi-level multimedia security": (i) "DB2 for z/OS encrypts a column using its native Column Level Encryption, and the table within which the encrypted column is embedded is itself encrypted using the IBM Encryption Tool for IMS and DB2 Databases"; and (ii) "DB2 for LUW encrypts a

---

<sup>12</sup> In fact, it appears that each of the six accused "infringing cases" is incapable of performing encryption at more than one level, as the accused products cannot nest encrypted objects within other encrypted objects. For example, in infringing case 1, the IBM Data Encryption Tool can only encrypt an entire table; it is incapable of nesting encrypted objects within other encrypted objects or providing multiple layers of encryption. Similarly, in infringing cases 2, 3, and 5, the built-in "column-level encryption" functionality of DB2 and IDS cannot nest encrypted objects within other encrypted objects. Finally, in infringing cases 4 and 6, the IBM Database Encryption Expert ("DEE") is only capable of encryption at the file level; it cannot nest encrypted objects and thereby provide multiple layers of data security. See Rjaibi Decl. [Dkt. No. 473] ¶¶ 6-8; Pickel Decl. [Dkt. No. 471] ¶¶ 7-9; Leffler Decl. [Dkt. No. 469] ¶¶ 7-8; Mandel Decl. [Dkt. No. 470] ¶¶ 9-13; Jackson Decl. [Dkt. No. 468] ¶¶ 6-9.

column using its built-in Column Level Encryption, and the tablespace in which the column is embedded is encrypted using IBM's Database Encryption Expert." See Pl.'s Br. in Opp. at 14. However, these additional hypothetical scenarios fail for the exact same reason that the other six failed: namely, because TecSec has produced no evidence that IBM's separate database products have ever been used together in the speculative configurations plaintiff identifies.<sup>13</sup> Moreover, TecSec has not cited any evidence showing that the two additional scenarios devised by its attorneys are capable of encrypting more than a single type of media, thereby failing to satisfy the required "multimedia" security element of the claims at issue. Accordingly, these alternative theories also fail as a matter of law.

b. The accused WebSphere products also do not provide "multi-level multimedia security."

TecSec has also failed to identify any evidence that IBM's accused WebSphere products provide multiple layers of encryption.<sup>14</sup> Indeed, as evidenced by the declaration of IBM engineer Shiu-Fun Poon, the WebSphere DataPower Appliances are not capable of providing the required "multi-level multimedia security" described

---

<sup>13</sup> The IBM Encryption Tool is not part of DB2 for z/OS, and the DEE is not part of DB2 for LUW. See Mandel Decl. [Dkt. No. 470]; see also Jackson Decl. [Dkt. No. 468].

<sup>14</sup> Once again, although TecSec was ordered to identify the source code supporting its infringement allegations, it provided no source code citation for its allegation that IBM's accused products infringe the "multi-level security" element of the asserted claims in the '702 (DCOM) patent family. See Dkt. No. 364 (Sept. 24, 2010 Order of Magistrate Judge Buchanan); see also Def.'s Ex. 16 at Ex. 9.

in the '702 family of patents. See Poon Decl. [Dkt. No. 472] ¶¶ 9-10. TecSec has failed to refute that declaration or to cite direct evidence in the record demonstrating that the accused DataPower Appliance products meet the claim limitations as construed by the Court. See Pl.'s Br. in Opp. at 14-15 (addressing only WAS, and not the WebSphere DataPower Appliance products).

Moreover, as explained by IBM engineer Hyen Chung, IBM's WebSphere Application Server ("WAS") product does not provide "multi-level multimedia security." See Chung Decl. [Dkt. No. 466] ¶¶ 8-9. TecSec's attorneys argue otherwise, contending that by using WAS, "an encrypted header may include encrypted data." See Pl.'s Br. in Opp. at 14. Specifically, TecSec's attorneys point to IBM documentation showing that when a message security header is encrypted using WAS, the "Encrypted Header" element contains an "Encrypted Data" element. Id. at 15. However, that argument is inapposite, as the WS-Security specification explains that the "Encrypted Data" element merely denotes the data resulting from encryption of the header, such that there is still only one level of encryption. See Def.'s Reply Br. at Ex. 48 ("The <wsse11:EncryptedHeader> element MUST contain the <xenc:Encrypted Data> produced by encrypting the header block."). Accordingly, because the cited evidence does not show multiple levels of encryption of multimedia, summary judgment of no infringement is appropriate in favor of IBM.



c. TecSec has provided no evidence of any single third party performing the entire act of alleged infringement with the accused WebSphere products.

To meet its burden of proving either direct or indirect infringement, a plaintiff must prove that a single party "practice[s] each and every element of the claimed invention." BMC Res., 498 F.3d at 1381. The independent method claims in the '702 patent family require, inter alia, that a single party perform the steps of: (i) "selecting an object"; (ii) "encrypting the object"; and (iii) "decrypting the object." See Def.'s Ex. 3 ('702 patent at claim 1, upon which claim 2 depends). The independent system claims, meanwhile, require a system with means for (i) "selecting an object"; (ii) "encrypting the object"; and (iii) "accessing the object." See id. (claim 12, upon which claims 14 and 15 depend). By the plain language of the claims, therefore, the method claims require that a single party both encrypt and decrypt the same object, and the system claims require that the system include a means for both encrypting and accessing the same object.<sup>15</sup>

However, TecSec has failed to come forward with any evidence that IBM or any third party directly infringes the '702 patent family by using or implementing the accused WebSphere products to both encrypt and decrypt or encrypt and access the same object. Indeed, the evidence in the record supports the conclusion that the accused WebSphere products cannot perform the claimed functionality

---

<sup>15</sup> Specifically, this issue applies to independent claims 1 and 12 of the '702 patent, claim 1 of the '781 patent, claim 1 of the '755 patent, and claim 1 of the '452 patent, as well as all claims dependent thereon.

as a matter of law because they are middleware products specifically designed to facilitate communications between two different parties. See Chung Decl. [Dkt. No. 466] ¶¶ 2-7; Poon Decl. [Dkt. No. 472] ¶¶ 2-8.

For example, by employing the accused WAS product, users can create and code their own web applications running on a server that a client device can access over a network. See Chung Decl. [Dkt. No. 466] ¶¶ 2, 5-7. A client, such as an end-user computer, may then send a message containing an "object" protected with the accused encryption functionality. Yet TecSec has produced no evidence that the same party ever implemented both the client and the server into an allegedly infringing configuration. Instead, the client simply performs the claimed steps of "selecting the object" and "encrypting the object," while the server hosting the web application service performs the claimed steps of "decrypting the object" or "accessing the object." Id. ¶¶ 6-7.

Similarly, in the WebSphere DataPower products, a client (such as an end-user computer) may send an encrypted message over the web to a server through the accused DataPower product, which decrypts the message before forwarding it to the destination server. See Poon Decl. [Dkt. No. 472] ¶¶ 6-8. Under that scenario, the client again performs the claimed "selecting the object" and "encrypting the object," and the DataPower product performs the claimed "decrypting the object" or "accessing the object." Id. There is simply no evidence in the record that the same party ever implemented the accused DataPower products to both encrypt and

decrypt the same object.

Accordingly, the accused WebSphere products have not both encrypted and decrypted the same object, as required by the '702 patent family. TecSec's attempt to overcome this fatal flaw in its infringement allegations by pointing to configurations involving multiple parties fails as a matter of law, because the actions of multiple parties cannot be combined to prove such infringement. See Cross Med. Prods., Inc. v. Medtronic Sofamor Danek, Inc., 424 F.3d 1293, 1311 (Fed. Cir. 2005) (rejecting a patentee's efforts to combine the acts of surgeons with the acts of the manufacturer to find infringement); see also BMC Res., 498 F.3d at 1381 (affirming summary judgment for the defendant because the patentee "chose . . . to have four different parties perform different acts within one claim" and "this court will not unilaterally restructure the claim or the standards for joint infringement to remedy these ill-conceived claims.").

In fact, plaintiff cannot establish that IBM or any third party directly infringed either the method claims or the system claims of the '702 patent family using IBM's WebSphere products. With respect to the method claims, TecSec argues that "IBM's literature confirms this WAS-WAS scenario in which both encryption and decryption/access steps are performed by a single party." See Pl.'s Br. in Opp. at 16. However, although the cited literature shows that two WAS systems can be connected, nothing in the IBM literature provides that both WAS systems are to be implemented by a single party. Moreover, none of the evidence cited by TecSec shows

that a single entity ever actually used the identified combinations of products to implement the accused encryption functionality, let alone to perform every claimed step of the asserted methods.<sup>16</sup> Finally, the figure identified by plaintiff, see id. at 17, clearly shows an additional device (the "browser"), suggesting that yet another independent party is required for TecSec's infringement theory to work. As such, there is no evidence that any single user ever directly infringed the asserted method claims in the '702 patent family.

Additionally, TecSec has also utterly failed to show that any single entity has ever assembled the various components of the allegedly infringing systems into the configurations that TecSec contends infringe the asserted system claims. Direct infringement by "use" of a system "requires a party . . . to use each and every . . . element of a claimed [system], and "[i]n order to 'put the system into service,' the end user must be using *all portions* of the claimed invention." Centillion, 2011 WL 167036, at \*4 (emphasis added) (internal citations omitted). As a result, even if some entity ever set up its system according to the specific infringing configurations identified by TecSec, there is no proof of infringement of the '702 (DCOM) patents because TecSec has not

---

<sup>16</sup> TecSec cites portions of testimony referring to terms such as "web services," but that is not the accused technology. Indeed, "web services" are not synonymous with "WS-Security," and a customer can implement "web services" without using "WS-Security," and can sometimes even use WS-Security without the accused WS-Security encryption. See, e.g., Chung Decl. [Dkt. No. 466] ¶¶ 4-5; Poon Decl. [Dkt. No. 472] ¶ 5.

identified any evidence that IBM or even IBM's direct customers ever initiated the communication that resulted in the accused encryption process.

Instead, at best, TecSec is limited to a highly attenuated indirect infringement theory involving end-users of the web "browser," i.e., the customers of IBM's customers. Such a theory is inadequate as a matter of law. See id. at \*5 (holding that defendant Qwest, as the operator of "back-end processing elements," could not infringe because the claimed invention required an end-user customer to initiate communications with the defendant's equipment). Indeed, not only has TecSec produced no evidence that anyone ever set up the particular accused configurations of systems at issue, it did not even raise an indirect system infringement theory based upon IBM's customers' end-users - and for good reason, because there is absolutely no evidence that IBM induced, or even *could* induce, the customers of its customers to do *anything*, let alone to infringe TecSec's patents.

4. The means-plus-function claims of the '702 patent have not been infringed as a matter of law.

Several of the asserted claims of the '702 patent read as means-plus-function claims. Patentees are permitted to express "[a]n element in a claim for a combination . . . as a means or step for performing a specified function." 35 U.S.C. § 112 ¶ 6. A patentee's choice of the word "means" in a claim "gives rise to a presumption that the inventor used the term advisedly to invoke the statutory mandates for means-plus-function clauses." Sage Prods.,

Inc. v. Devon Indus., Inc., 126 F.3d 1420, 1427 (Fed. Cir. 1997) (internal citations and quotations omitted).

In this case, the '702 patentee drafted a number of the limitations of claims 8-9 and 12-15 in that means-plus-function format. See Def.'s Ex. 3 at 12:45-49 (independent claim 8, upon which claim 9 depends, describing a "digital logic means" and "system memory means"); id. at 13:20-22 (dependent claim 9, further claiming a "means for embedding a first object within a second object"); see also id. at 14:3-15 (independent claim 12, upon which claim 15 depends, describing "means for" "selecting an object to encrypt," "selecting a label for the object," "selecting an encryption algorithm," "encrypting the object," "labelling [sic] the encrypted object," "reading the object label," "determining access authorization based on the label," and "accessing the object if access authorization is granted"); id. at 14:25-30 (dependent claim 15, further claiming "means for reading the second object label," "means for determining access authorization based on the second object label," and "means for decrypting the second object if access authorization is granted.")).

However, because TecSec failed to identify sufficient corresponding structure for each of those means-plus-function limitations, and failed to compare the corresponding structure to any allegedly equivalent structure in IBM's accused systems, plaintiff's allegations of infringement of those claims fail as a matter of law. See CytoLogix Corp. v. Ventana Med. Sys., Inc., 424 F.3d 1168, 1178 (Fed. Cir. 2005).

a. TecSec has not identified sufficient supporting structure for the means-plus-function claims.

In construing means-plus-function terms, the "court must identify both the claimed function and the corresponding structure in the written description for performing that function." Wenger Mfg., Inc. v. Coating Mach. Sys., Inc., 239 F.3d 1225, 1233 (Fed. Cir. 2001). "In order to qualify as corresponding, the structure must not only perform the claimed function, but the [patent] specification must clearly associate the structure with performance of the function." Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 296 F.3d 1106, 1113 (Fed. Cir. 2002). "This duty to link or associate structure to function is the quid pro quo for the convenience of employing § 112, ¶ 6." B. Braun Med., Inc. v. Abbott Labs, 124 F.3d 1419, 1424 (Fed. Cir. 1997).

Although the '702 patent's means-plus-function claims explicitly recite the claimed functions, such as "accessing an object-oriented key manager," or "embedding a first object within a second object," see Def.'s Ex. 3 at 14:3-4; id. at 13:21-22, the '702 patent fails to identify adequate corresponding structures for performing each of those functions, and there is nothing in the patent specification that "clearly links" any structure to any of the claimed functions, as is required by Federal Circuit law. See Default Proof Credit Card Sys., Inc. v. Home Depot U.S.A., Inc., 412 F.3d 1291, 1298 (Fed. Cir. 2005) ("A structure disclosed in the specification qualifies as 'corresponding' structure only if the specification or prosecution history clearly links or associates

that structure to the function recited in the claim." ). Moreover, when asked during discovery to identify the corresponding structure for performing each of the claimed functions, TecSec was unable to do so. See Def.'s Ex. 11 at 2-3 (TecSec's response to IBM's Interrogatory No. 19, identifying no support for each asserted means-plus-function claim limitation).

TecSec's counsel now asserts that the '702 patent recites sufficient structural terms to overcome any means-plus-function presumption, pointing to terms such as "an object labelling [sic] system," "electronically connected," "system memory means," "accepting inputs," "an encryption algorithm module," "a decryption algorithm module, and "an object label identification subsystem." See Pl.'s Br. in Opp. at 18. However, none of those "structural" elements - to the extent they even constitute structure at all - is part of the "digital logic means" claim limitation, nor does the '702 patent ever clearly associate that asserted "structure" with performance of any of the specific functions claimed. See Def.'s Ex. 3 at 12:56-64. Furthermore, TecSec's suggestion that the "object labelling [sic] subsystem" is structure for the "logic means" is unfounded as a matter of law. See NetMoneyIN, Inc. v. Verisign, Inc., 545 F.3d 1359, 1366 (Fed. Cir. 2008) (rejecting, as "both redundant and illogical," a patentee's argument that "first bank computer" in "first bank computer including means for generating authorization indicia" somehow recites sufficient structure for the claimed function of "generating authorization indicia"). Finally, the Federal Circuit has squarely held that



computer-implemented means-plus-function limitations, such as those at issue here, are, by definition, limited to the algorithm disclosed in the specification for performing the claimed functions. See Harris Corp. v. Ericsson Inc., 417 F.3d 1241, 1253 (Fed. Cir. 2005); see also Aristocrat Techs. Austl. Pty Ltd. v. Int'l Game Tech., 521 F.3d 1328, 1337 (Fed. Cir. 2008). Yet the '702 patent specifications disclose no such algorithms. Accordingly, the means-plus-function claims in the '702 patent lack sufficient corresponding structure.

b. TecSec has not established that any of IBM's accused products infringe the asserted means-plus-function claims.

Even if TecSec could identify sufficient corresponding structure to support the asserted means-plus-function claims in the '702 patent, to prove infringement of those claims, TecSec must also show that the defendant's accused products perform the recited functions with structure that is the same as or equivalent to the corresponding structure in the '702 patent specification. See Baran v. Med. Device Techs., Inc., 616 F.3d 1309, 1316-17 (Fed. Cir. 2010). However, neither TecSec nor its experts has adequately identified or compared the '702 patent's asserted structure with any of the structures of IBM's accused products. Specifically, although TecSec has identified certain structural elements of the accused products which it claims correspond to the structures described in the '702 patent, it has not sufficiently explained how those structures are identical or equivalent, even if they perform similar functions. This failure is fatal to TecSec's infringement claims

and precludes any finding of infringement as a matter of law:

Infringement of a means-plus-function limitation "requires that the relevant structure in the accused device . . . be identical or equivalent to the corresponding structure in the specification." To establish infringement under § 112, ¶ 6, it is insufficient for the patent holder to present testimony "based only on a functional, not a structural, analysis." Here, [plaintiff] failed to identify the structure in the specification that is the "temperature controller means" and compare it to the structure of the accused device. Accordingly, because [plaintiff] failed to present substantial evidence of infringement of claim 13 of the '693 patent, the jury verdict of infringement of claim 13 must be reversed.

CytoLogix, 424 F.3d at 1178 (citations omitted); see also Alpex Computer Corp. v. Nintendo Co., 102 F.3d 1214, 1222 (Fed. Cir. 1996) (finding no infringement because the plaintiff's expert "did not compare the structure of the [accused product] with the bit map structure disclosed in the specification."). Accordingly, on this record, the infringement allegations relating to the means-plus-function claims of the '702 patent fail as a matter of law.

#### C. '433 (XML) Patent

TecSec also asserts that various IBM products infringe independent method claims 1 and 3, dependent method claims 8 and 12, and system claim 4 of the '433 patent, which covers an "XML encryption scheme" whereby "process elements are provided to a process," such as an Extensible Markup Language ("XML"), "selected elements are manipulated," tagged, labeled, and selected based upon their XML label or tag, "and the process sample is encrypted to provide an encrypted output." See Def.'s Ex. 12 ('433 patent) at Abstract; see also id. at 5:13-48 (detailed description of the

invention, describing it "in terms of a particular process, that is, the Extensible Markup Language (XML)". For example, independent method claim 1 of the '433 patent claims:

A method, comprising:

providing, consistent with a data format, at least one object relating to a process;

selecting, from the at least one object, a first object having an object tag associated therewith, wherein the first object is an Extensible Markup Language element;

encrypting at least a portion of the first object according to at least one cryptographic scheme determined at least in part by the object tag; and

storing the encrypted at least a portion [sic] of the first object for subsequent use by an intended recipient.

Id. at 6:62-7:6.

Based on the Court's construction of the term "storing" in the '433 patent, along with TecSec's failure to provide sufficient evidence of infringement of that patent, summary judgment is appropriate in IBM's favor on plaintiff's allegations of infringement.

#### 1. Claim Construction: "Storing"

The '433 patent specification explains in detail how the objects of the claimed invention may be handled after they are selected and encrypted. Specifically, the specification describes either passing those objects directly to the proper authorized recipients, or storing and forwarding them at a later time:

The encrypted objects are then either passed directly on a real-time basis to authorized recipients for immediate decryption and further processing, or they are stored and forwarded at a later time. . . . Each

input object copy is encrypted and passed to or stored for appropriate persons, devices, or other systems.

Def.'s Ex. 12 ('433 patent) at 5:46-49; 5:67-6:3; see also id. at 6:20-24; 6:56-60.

However, the asserted claims themselves cover only the "storing" alternative; indeed, every independent claim of the '433 patent requires "storing" the encrypted information. See, e.g., id. at 7:4-5 (claim 1, describing "storing . . . at least a portion of the first object for subsequent use by an intended recipient"); id. at 7:28-30 (claim 3, describing "storing . . . at least a portion of the first object and the object tag for subsequent use by an intended recipient"); id. at 7:43-44 (claim 4, describing "storing . . . at least a portion of the first object for subsequent use by an intended recipient.").<sup>17</sup>

The other alternative described in the patent specification - passing the information on a real-time basis to intended recipients - is not mentioned in any of the claims and must be deemed dedicated to the public. Accordingly, as a matter of law, the patent claims at issue in this action cannot be interpreted to cover that alternative. See Unique Concepts, Inc. v. Brown,

---

<sup>17</sup> The asserted dependent method claims in the '433 patent, claims 8 and 12, also depend upon independent claims which themselves require "storing" an object or data set. For example, independent claim 7, upon which claim 8 depends, requires "storing [a] data set on one of the first computer readable medium and a second computer readable medium." Def.'s Ex. 12 ('433 patent) at 8:28-30. Similarly, independent claim 10, upon which claim 12 depends, describes "storing the encrypted [] object on the one of said first computer readable medium and the second computer readable medium." Id. at 8:53-55.

939 F.2d 1558, 1562-63 (Fed. Cir. 1991) ("It is also well established that subject matter disclosed but not claimed in a patent application is dedicated to the public"); see also PSC Computer Prods., Inc. v. FoxConn Int'l, Inc., 355 F.3d 1353, 1360 (Fed. Cir. 2004) ("The disclosure-dedication rule requires an inventor who discloses specific matter to claim it, and to submit the broader claim for examination. Otherwise, that matter is dedicated to the public.").

The parties in this case agree that, at a minimum, "storing" requires "transferring information to (or retaining information in) a device from which it can be obtained at a later time." See Def.'s Reply Br. at 18. In fact, IBM proposes exactly that construction of "storing," and TecSec's only proposed alteration to that definition is to suggest that "storing" be construed as "transferring information to (or retaining information in) a device *such as memory or disk* from which it can be obtained at a later time." See id.; see also Pl.'s Br. in Opp. at 22 (emphasis added).

IBM's proposed definition is fully consistent with the ordinary and customary meaning of the term "store," which is defined as "[t]o transfer an element of information to a device from which the unaltered information can be obtained at a later time" or "[t]o retain data in a device from which it can be obtained at a later time." See Def.'s Ex. 13 (Charles J. Sippl, Computer Dictionary (4th Ed.)) at 478; see also Def.'s Ex. 14 (The American Heritage Dictionary) at 1201. IBM's construction

also comports with the intrinsic evidence and the other language of the '433 patent claims. For example, claims 1-6 of the '433 patent expressly require "storing . . . *for subsequent use*," and claims 7 and 10 require "storing" on a "computer readable medium." See Def.'s Ex. 12 (emphasis added). The context in which the term "storing" is used in the '433 patent claims thus supports adoption of the ordinary and customary meaning of that term.

By contrast, TecSec's proposed construction would impermissibly define the term "storing" out of the '433 patent. Under plaintiff's proposed construction, the fleeting presence of information in memory while that information is being encrypted and transmitted to a recipient would somehow constitute "storing" the information for subsequent use. That interpretation is contrary to the ordinary meaning of "storing" and would erase the patentee's clear differentiation in the patent specification between "storing" and "passing [information] directly on a real-time basis." See Def.'s Ex. 12 at 5:46-49. Accepting TecSec's definition would also mean that the "storing" limitation adds nothing to the claims, as it would then be literally impossible to encrypt and transmit information without also simultaneously "storing" it.

For those reasons, TecSec's proposed construction must be rejected, see Tex. Instruments, 988 F.2d at 1171 (rejecting a construction that "would read an express limitation out of the claims"), and the Court will construe "storing" in the '433

patent to mean "transferring information to (or retaining information in) a device from which it can be obtained at a later time."

2. The accused WebSphere products do not perform the claimed "storing" functionality.

On the record before the Court, there is no genuine dispute that IBM's accused WebSphere products do not "store" encrypted information during the accused functionality, and therefore do not infringe the '433 patent. In fact, the evidence indicates that the WebSphere products are not capable of storing encrypted messages, but instead are designed to pass encrypted messages along on a real-time basis, as quickly as possible, to the intended recipients for immediate decryption. See Chung Decl. [Dkt. No. 466] ¶ 11 ("During a web-services transaction, WAS does not permanently hold any portion of the message encrypted with WS-Security. WAS does not retain any portion of the encrypted message such that the encrypted message can be obtained at a later time. During WS-Security processing, WAS is designed to process the message as fast as possible and then send the message to the intended recipient immediately."); see also Poon Decl. [Dkt. No. 472] ¶¶ 14-15. The functionality provided by the accused WebSphere products is therefore precisely what the '433 patent *distinguished* from "storing" and ultimately did not claim. See Def.'s Ex. 12 at 5:45-49 ("The encrypted objects are then either passed directly on a real-time basis to authorized recipients for immediate decryption and further processing, or they are stored

and forwarded at a later time.") (emphasis added); see also id. at 6:1-3; 7:4-5.

Plaintiff's primary argument in response is that the WebSphere products use "system memory," and that the system memory briefly retains the encrypted information as it is being processed.<sup>18</sup> TecSec again argues that the use of such memory constitutes "storing" and therefore provides sufficient foundation for its infringement contentions. However, as explained above, the accused products' use of memory cannot qualify as "storing," at least as that term is used by the '433 patentee. Accordingly, because TecSec's infringement allegations attempt to encompass embodiments that are not actually claimed by the '433 patent, plaintiff's allegations fail as a matter of law. See Schoenhaus v. Genesco, Inc., 440 F.3d 1354, 1359 (Fed. Cir. 2006) (finding a disclosed but not claimed feature "dedicated to the public" and affirming the district court's grant of summary judgment of no infringement); Maxwell v. J. Baker, Inc., 86 F.3d 1098, 1107 (Fed. Cir. 1996) (prohibiting a finding of infringement "when an accused infringer practices disclosed but unclaimed subject matter.").

---

<sup>18</sup> TecSec's expert also identified a feature called a "Message Store" for the WebSphere Application Server (WAS) product, claiming that it meets the "storing" limitation. The Message Store feature, however, does not perform the required functionality because it stores only unencrypted messages, not encrypted messages, as required by the patent claims. See, e.g., Def.'s Ex. 12 at 7:4-5.



3. Plaintiff admits that the accused DataPower Appliance products do not meet the "providing" limitation.

The only product on which IBM did not explicitly move for summary judgment in its favor regarding the "storing" limitation of the '433 patent is the DataPower XB60 product. See Def.'s Mot. for Summ. J. at 26 n.13. However, plaintiff's infringement allegations relating to that product fail for another, independent reason: namely, TecSec has conceded that that product does not "provid[e]" the required data objects, as claimed in the '433 patent.

Every independent claim of the '433 patent requires "providing . . . at least one object relating to a process" or "providing a first computer readable medium having stored thereon a first data set." See Def.'s Ex. 12 (claims 1-7, 10). There is no dispute between the parties that IBM's accused DataPower Appliance products, including the DataPower XB60 product, do not perform that required step. Indeed, TecSec's expert has not articulated any possible theory under which the DataPower Appliance products "provide" data to be encrypted, and TecSec's Memorandum in Opposition to IBM's Motion for Summary Judgment addressed only the WebSphere Application Server, thereby admitting that the DataPower Appliance products, such as DataPower XB60, cannot "provide" an object or a first computer readable medium having stored thereon a first data set. See Pl.'s Br. in Opp. at 21-22 (addressing only the WebSphere Application Server); see also Stubblebine Decl. [Dkt. No. 509] ¶¶ 19-21 (same). Summary

judgment of no infringement of the '433 patent is therefore appropriate on that basis, as well.

**D. '448 (Parallel Processor) Patent**

TecSec alleges that when IBM's System z9 and z10 mainframe servers are configured with encryption "cards," called "CryptoExpress2" and "CryptoExpress3," they infringe the '448 patent, which covers "context-oriented crypto-processing on a parallel processor array." See Def.'s Ex. 15 ('448 patent). Specifically, TecSec asserts infringement of independent system claim 1 in the '448 patent, and its dependent claim 5. Claim 1 describes:

A system for cryptographic processing of input data on a parallel processor array that includes a plurality of processors, comprising

a format filter adapted to extract control data and main data from the input data;

a control unit adapted to receive the control data from said format filter, and to forward, based at least in part on the control data, at least one respective control parameter and at least one respective cryptographic parameter to each of the plurality of processors;

a first distributor adapted to receive the main data from said format filter, and to distribute to each of the plurality of processors a respective at least [sic] a portion of the main data;

a second distributor adapted to receive respective output information from each of the plurality of processors, and to generate, based at least in part on the respective output information, output data;

wherein each of the plurality of processors is adapted to generate its respective output information based at least in part on the control parameters and the cryptographic parameters, and the output data is a cryptographic processing result.

Id. at 6:26-48. Dependent claim 5 requires "[t]he system of claim 1, wherein each respective at least a portion [sic] of the main data is a multiplexed process stream." Id. at 6:56-57.

IBM is entitled to summary judgment on plaintiff's allegations of infringement of the '448 patent because TecSec has failed to come forward with any evidence that the accused System z products include a "format filter adapted to extract control data and main data from the input data," as claimed in both claim 1 and claim 5 of the '448 patent.

1. Claim Construction: "Extract"

As explained above, both asserted claims of the '448 (Parallel Processor) patent require, inter alia, a "format filter adapted to extract control data and main data from the input data." See id. at 6:29-30 (claim 1); id. at 6:56-57 (claim 5, which depends on claim 1). IBM proposes a construction of "extract" as "separate out," such that "to extract control data and main data from the input data" means "to separate out control data and main data from the input data." See Def.'s Mot. for Summ. J. at 27, 30. TecSec did not specifically offer a competing construction of "extract" in the '448 patent, but maintains that "[i]n the context of the ['448 patent] claims, extract refers to the process of separating the control data and the main data." See Def.'s Ex. 29 (Buroker Declaration).

IBM's construction is clearer and more accurately reflects the '448 patent's requirement that the claimed system be able to

"extract control data and main data *from the input data*," Def.'s Ex. 15 at 6:29-30 (emphasis added), rather than simply separating the control data and main data from each other. IBM's construction also plainly adheres to the common and ordinary meaning of the word "extract." Accordingly, the Court will construe "extract control data and main data from the input data" in the '448 patent to mean "separate out control data and main data from the input data."

2. The accused products do not meet the "format filter adapted to extract . . ." limitation.

The '448 patent requires that a structure called the "format filter" be "adapted to extract control data and main data from the input data." Id. The only structure that plaintiff has identified in IBM's products that allegedly corresponds to the claimed "format filter" is something called the "Integrated Cryptographic Service Facility" ("ICSF"), which essentially functions as an interface program between the System z mainframe and the particular CryptoExpress feature that is being employed. See Pl.'s Br. in Opp. at 26-27.

Contrary to plaintiff's assertions, however, the record evidence demonstrates that the ICSF does not perform the claimed functionality. Specifically, the ICSF does not "extract," or separate out, control data and main data from input data; rather, as TecSec admits, the ICSF actually *combines* all data relating to a particular processing request into a single data structure so that it can be sent to the cryptographic processing "card" for

encryption. See id. at 27 ("[T]he ICSF takes a request from an application program, take[s] the parameters, and put[s] them into a data structure . . . to send down to the hardware of the cryptographic coprocessor card.").

TecSec nonetheless contends that the extracting limitation is met because the ICSF reformats the data into "a CPRB block" and a "parameter block," which allegedly correspond to the main data and control data. However, plaintiff's theory as to how the ICSF functions is internally inconsistent: for example, TecSec claimed in its briefing and its expert reports that the CPRB block corresponds to the main data, while the parameter block corresponds to the control data, but at oral argument, TecSec's counsel argued just the opposite. Compare id. at 26 ("The ICSF . . . reformats data into a structure that includes: (1) a CPRB block (main data) and (2) parameter block (control data), with pointers to the separate data") (citing Rubin Decl. [Dkt. No. 508] ¶¶ 9-22) to Tr. of Mot. Hr'g (Feb. 11, 2011) at 87-88 (arguing that the control information is in the CPRB block, while "[t]he main data is put in the parameter block").

Moreover, regardless of which type of data corresponds to the main data or control data, TecSec's infringement theory fails because the undisputed evidence reveals that the ICSF simply does not perform the claimed functionality. First, the "parameter block," as reformatted by the ICSF, includes both main data (which is the data to be processed and encrypted), and various forms of control data, including the request-type key ID and cryptographic

keys. See Def.'s Reply Br. at Exs. 50-51; see also Arnold Decl. [Dkt. No. 465] ¶¶ 8-9. The ICSF self-evidently cannot perform the required extraction, or separation, of control and main data if those two forms of data are still mixed together in a single data block even after the ICSF has allegedly reformatted the input data.

Additionally, even the evidence submitted by TecSec reveals that the ICSF does not function as a "format filter," as claimed in the '448 patent. In particular, plaintiff admits that the "CPRB block" and "parameter block" are "concatenated," or appended together, in a data structure that is then sent to the CryptoExpress2 or CryptoExpress3 processor as a single unit. See Rubin Decl. [Dkt. No. 508] ¶ 16-18 (acknowledging that the CPRB block and the parameter block are "appended" to one another). The result is therefore a "single contiguous block" of data to be processed together by the same cryptographic "card" processor. See Def.'s Ex. 50 at 21; see also id. at 39 ("When the data is transferred to or from the XCrypto card, the CPRB, parameter block, and parameter extension are concatenated to form a single block of data."); Arnold Decl. [Dkt. No. 465] ¶ 8 (showing a diagram of the CPRB block "concatenated with several other blocks"). Even under TecSec's theory, therefore, the ICSF does not separate control data and main data from the input data, and the control and main data therefore cannot be sent separately to a "control unit" and "first distributor," respectively, as required by the '448 patent. See Def.'s Ex. 15 at 6:32-37 (claiming a

"control unit adapted to receive the control data" and a "first distributor adapted to receive the main data").

Because the accused IBM products perform the exact opposite of the claimed "extract[ion]" step in the '448 patent, by actually combining or uniting control data and main data, IBM is entitled to summary judgment of no infringement as a matter of law on all of plaintiff's '448 patent claims. See, e.g., Planet Bingo, LLC v. GameTech Int'l, Inc., 472 F.3d 1338, 1345 (Fed. Cir. 2006) (refusing to find infringement in "cases where the accused device contained the antithesis of the claimed structure.").

#### IV. Conclusion

In sum, after conducting extensive discovery, including subpoenaing a wide variety of IBM's customers to determine whether any of them ever used any of IBM's products in an infringing fashion, and gaining access to IBM's source code, plaintiff has failed to uncover any actual evidence of direct infringement by IBM or any of its customers. Accordingly, summary judgment is appropriate in the defendant's favor on all infringement claims.

For all these reasons, defendant IBM's Motion for its Proposed Claim Constructions and Summary Judgment of No Infringement [Dkt. No. 462] has been granted, plaintiff TecSec's Motion for Partial Summary Judgment of Infringement by Defendant IBM and on Defendant's Affirmative Defenses of Release and Immunity under 28 U.S.C. § 1498 [Dkt. No. 478] has been denied,<sup>19</sup>

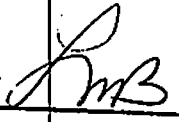
---

<sup>19</sup> Because the parties were preparing for an imminent trial date, the Court announced its decision on the parties' cross-motions in an Order issued on February 25, 2011.

and summary judgment will now be entered in favor of defendant IBM by an Order to be issued with this Memorandum Opinion.

Entered this 3<sup>rd</sup> day of March, 2011.

Alexandria, Virginia

/s/   
Leonie M. Brinkema  
United States District Judge